Privacy Awareness Week 2024

Hamilton Locke

It’s time to power up your privacy

Hamilton Locke is proud to support the Office of the Australian Information Commissioner’s 2024 Privacy Awareness Week (PAW).

This year’s theme of ‘power up your privacy’ encourages businesses, organisations and individuals to consider steps that can be taken to enhance transparency, accountability and security.

Data-driven technology is providing promising advances for both the private and public sectors. However, in this environment where data is being captured constantly, Australian Privacy Commissioner Carly Kind highlights that most Australians want to have greater power over their personal information.

The message to businesses is clear: to support consumer trust, the right decisions must be made to adequately protect and respect data and steps must be taken to ensure that privacy practices are fit for purpose.

While the precise detail of the long-awaited reforms to the Privacy Act is not yet known, there are are clear signs from the Government that it supports significant reform to the Privacy Act (albeit, not in the short-term). This “political will” for reform, combined with increased community expectations and regulator enforcement activity, means organisations should take steps now to “power up” their privacy practices.

How can your business improve its privacy practices?

The Federal Government’s response to the proposed reforms to the Privacy Act indicated clear support for significant reform. If enacted as proposed, these reforms would significantly impact information-handling practices of private and public sector entities.

The Government has indicated that it is committed to introducing amending legislation in 2024 to address the 38 “agreed” proposals for law reform. We’ve unpacked five of the key reforms agreed by the Government on the following page.

In the mean time, organisations can (and should) start to prepare now, including taking steps to:

1. Understand what personal information the organisation holds, where and how. This includes where personal information is held or otherwise handled by third party service providers.

2. Understand current information handling practices and how the organisation currently complies with its obligations under the Privacy Act. A privacy compliance audit or maturity assessment is a useful exercise to identify any gaps and other compliance and privacy risks.

3. Develop and implement a roadmap to uplift the organisation’s existing privacy management framework. This will include updating practices, procedures and systems and conducting a privacy awareness program. This roadmap should include key reforms that would impact the organisation, privacy awareness and training requirements, and projected future resourcing requirements.

Five key proposed reforms to the Privacy Act anticipated in 2024

1. Security obligations to be clarified

The Privacy Act currently requires regulated entities to take steps that are reasonable in the circumstances to protect personal information and to destroy or de-identify it once it is no longer needed or required to be retained, unless an exception applies.

In order to provide further certainty for organisations, the Government agrees with the proposal for the OAIC to provide enhanced guidance as to what constitutes "reasonable steps" and to amend APP 11.1 to specify that reasonable steps to protect personal information includes both technical and organisational measures.

2. Privacy Impact Assessment for "high risk" practices

There is currently an obligation under the Privacy Act for an organisation to take steps that are 'reasonable in the circumstances' to implement practices, procedures and systems that ensure the organisation complies with the Australian Privacy Principles (APPs) and applicable APP code.

This will include, where appropriate, conducting a Privacy Impact Assessment (PIA), however, this is not currently prescribed.

While the Government has indicated its support to require PIAs to be conducted for high risk practices, it has not as yet agreed to this being a mandatory requirement generally.

The Government does agree, however, to further consider enhanced risk assessment requirements where facial recognition technology and other uses of biometric information, as part of the broader consideration by Government of the regulation of biometric technologies.

3. Accountability through enhanced enforcement and other regulatory powers

The majority of the "agreed" reforms are to enhance existing regulatory enforcement powers and processes, in addition to those reforms included as part of the 2022 amendments to the Privacy Act.

These include clarification of what constitutes a "serious" interference with privacy, introduction of new civil penalty tiers and empowering the Privacy Commissioner to make a determination following an investigation.

The Government also agrees to amend the Privacy Act to better facilitate the sharing of information in the event of an eligible data breach to reduce risk of harm, with appropriate controls.

Five key proposed reforms to the Privacy Act anticipated in 2024

4. Strengthening of children's privacy

Currently, the Privacy Act does not distinguish between adults and children.

It also does not specify an age at which individuals can make their own privacy decisions (other than where consent to the information handling is required under the APPs, in which case the question of age is a consideration in terms of the individual's capacity to consent).

The Government agrees to amend the Privacy Act to define a "child" as an individual who has not reached 18 years of age and to develop a "Children's Online Privacy Code" to address how the best interests of a child should be taken into account in the design of an online service.

This code will align with the UK's Age Appropriate Design Code and be developed in consultation with the Australian eSafety Commissioner, children, parents, industry and other experts.

5. Transparency on automated decision making

The Government agrees that privacy policies should outline the types of personal information that will be used in "substantially automated decisions" which have a legal or similarly significant effect on an individual's rights.

It also agrees that the Privacy Act (supplemented by OAIC guidance) should provide high level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights.

The Government also agrees to giving individuals a right to request meaningful and clear information (free of jargon) about how automated decisions are made that have a legal or similarly significant effect on their rights.

These "agreed" reforms to the Privacy Act are similar to those contained in the EU General Data Protection Regulation and are in the context of the Government's comments and feedback received during consultation of the importance of organisations and government using automated decision making in a safe and responsible way, and with transparency and integrity.

These proposals are proposed to be implemented as part of the Government's broader review of the regulation of AI and automated decision-making.

For more information about the Government's response to the proposed reforms, or on uplifting your organisation's privacy practices, please contact a member of the Hamilton Locke Cyber & Privacy team.

Get in Touch

Sophie Bradshaw
Partner
sophie.bradshaw@hamiltonlocke.com.au
+61 450 903 631

View Profile

Sarah Gilkes
Partner
sarah.gilkes@hamiltonlocke.com.au
+61 422 229 461

View Profile

Janice Yew
Senior Associate
janice.yew@hamiltonlocke.com.au
+61 430 430 036

View Profile

Ben Cameron
Special Counsel
ben.cameron@hamiltonlocke.com.au
+61 405 135 939

View Profile

Verity Stone
Senior Associate
verity.stone@hamiltonlocke.com.au
+61 432 468 832

View Profile

Adam Rose
Lawyer
adam.rose@hamiltonlocke.com.au
+61 481 089 007

View Profile

Isabel Roach
Lawyer
isabel.roach@hamiltonlocke.com.au
+61 431 652 472

View Profile